

Jan Camenisch • Simone Fischer-Hiibner
Kai Rannenberg
Editors

Privacy and Identity Mangement for Life

4y Springer

Contents

Introduction

1	PrimeLife	5
	Andreas Pfitzmann, Katrin Borcea-Pfitzmann, and Jan Camenisch	
1.1	Motivation	5
1.2	Vision and Objectives of the PrimeLife Project	7
1.3	Defining Privacy	8
1.4	From Identity via Identity Management to Privacy by Identity Management	9
1.4.1	Identity - What it is	10
1.4.2	Presentation of Identities - Pseudonyms	13
1.4.3	Time Aspects of Identity Management and Privacy.	17
1.5	Further Facets of Privacy	19
1.6	PrimeLife's Contributions to Protect Privacy	20
1.6.1	Part I - Privacy in Life	22
1.6.2	Part II - Mechanisms for Privacy	22
1.6.3	Part HJ - Human Computer Interaction (HCI)	23
1.6.4	Part IV - Policy Languages	24
1.6.5	Part V- Infrastructures for Privacy and Identity Management.	25
1.6.6	Part VI- Privacy Live	25
	References Introduction	27

Part I Privacy in Life

2	Privacy in Social Software	33
	Bibi van den Berg, Stefanie Potzsch, Ronald Leenes, Katrin Borcea-Pfitzmann, and Filipe Beato	
2.1	Scenarios and Requirements	33
2.1.1	Scenario 1: A Social Network Site	35
2.1.2	Scenario 2: A Forum	36

2.1.3	General Requirements	36
2.2	Two Prototypes for Privacy-Enhanced Social Networking	37
2.2.1	Introduction	37
2.2.2	Privacy Issues in Social Network Sites	38
2.2.3	Clique: An Overview	42
2.2.4	Scramble!: An Overview	46
2.3	Privacy-Enhancing Selective Access Control for Forums	50
2.3.1	Objectives	50
2.3.2	Introducing phpBB Forum Software and PRIME Framework	51
2.3.3	Extending phpBB with Selective Access Control	52
2.3.4	Scenario Revisited	54
2.3.5	Privacy-Awareness Information	55
2.3.6	User Survey	55
2.4	Concluding Remarks	59
2.5	Acknowledgements	60
	Trustworthiness of Online Content	61
	Jan Camenisch, Sandra Steinbrecher, Ronald Leenes, Stefanie Potzsch, Benjamin Kellermann, and Laura Klaming	
3.1	Introduction	61
3.2	Scenarios and requirements	63
3.2.1	Scenarios	63
3.2.2	High-level mechanisms	65
3.2.3	Requirements of mechanisms	66
3.3	Experiments	70
3.3.1	Binding metadata to data	71
3.3.2	User Reputation and Certification	74
3.4	Demonstrators	76
3.4.1	Trustworthy Blogging	76
3.4.2	Encouraging Comments with Incentives	78
3.4.3	Author reputation system and trust evaluation of content in MediaWiki	80
3.5	Conclusive Remarks	84
3.6	Acknowledgements	85
	Identity and Privacy Issues Throughout Life	87
	Jaromir Dobias, Marit Hansen, Stefan Kopsell, Maren Raguse, Arnold Roosendaal, Andreas Pfitzmann, Sandra Steinbrecher, Katalin Storf, and Harald Zwingelberg	
4.1	Challenges and Requirements	87
4.1.1	Dealing with Dynamics	87
4.1.2	Digital Footprint	91
4.1.3	Concepts for Delegation	94
4.2	Demonstrator	99
4.2.1	Overview of the Backup Demonstrator Architecture	102

4.2.2	Deployment and Usage of the Demonstrator.	109
4.3	Concluding Remarks.	110
4.4	Acknowledgements.	110
References Part I.		111
Part II Mechanisms for Privacy		
5	Cryptographic Mechanisms for Privacy.	117
	Jan Camenisch, Maria Dubovitskaya, Markulf Kohlweiss, Jorn Lapon, and Gregory Neven	
5.1	Introduction.	117
5.2	Cryptography to the Aid.	118
5.3	Private Credentials, Their Extensions, and Applications.	119
5.3.1	Extended Functionalities.	120
5.3.2	Direct Anonymous Attestation.	123
5.4	Other Privacy-Enhancing Authentication Mechanisms.	123
5.4.1	Privacy-Enhancing Encryption.	126
5.5	Electronic Voting, Polling, and Petitions.	127
5.6	Oblivious Transfer with Access Control and Prices.	128
5.7	Oblivious Trusted Third Parties.	130
5.8	Conclusion.	134
6	Transparency Tools.	135
	Hans Hedbom, Tobias Pulls, and Marit Hansen	
6.1	Introduction.	135
6.2	Setting the Scene.	137
6.3	On Privacy Preserving and Secure Logs.	138
6.3.1	Attacker Model and Security Evaluation.	139
6.4	Prior Work and Our Contribution.	139
6.5	Technical Overview.	140
6.5.1	State and Secrets.	140
6.5.2	Entry Structure and Storage.	141
6.5.3	API.	142
6.5.4	Unlinkability.	142
6.6	Conclusion and Outlook.	143
7	Interoperability of Trust and Reputation Tools.	145
	Sandra Steinbrecher and Stefan Schiffner	
7.1	Introduction.	145
7.2	Social need.	146
7.3	Legal Aspect.	147
7.4	Security and Privacy Requirements.	148
7.5	Technical Implementability.	149
7.6	Infrastructure.	150
7.6.1	Interoperability with Applications.	150

7.6.2	Interoperability with Trust Management152
7.6.3	Interoperability with Identity Management153
7.6.4	Resulting implementation154
7.7	Conclusion155
8	Data Privacy157
	Michele Bezzi, Sabrina De Capitani di Vimercati, Sara Foresti, Giovanni Livraga, Stefano Paraboschi, and Pierangela Samarati	
8.1	Introduction157
8.2	Privacy Metrics and Information Theory158
8.2.1	Basic Concepts159
8.2.2	Traditional Privacy Metrics160
8.2.3	An Information Theoretic Approach for Privacy Metrics161
8.2.4	Protecting Privacy of Sensitive Value Distributions164
8.3	Privacy Protection Techniques165
8.3.1	Basic Concepts165
8.4	Fragmentation and Encryption167
8.4.1	Fragmentation Model168
8.4.2	Minimal Fragmentation169
8.4.3	Query Evaluation170
8.5	Departing from Encryption171
8.5.1	Fragmentation Model172
8.5.2	Minimal Fragmentation172
8.5.3	Query Evaluation174
8.6	Preserving Utility in Data Publication175
8.6.1	Visibility Requirements175
8.6.2	Loose Associations176
8.7	Conclusions179
9	Selective Exchange of Confidential Data in the Outsourcing Scenario181
	Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, Gerardo Pelosi, and Pierangela Samarati	
9.1	Introduction181
9.2	Preliminaries183
9.3	Encryption Schema184
9.3.1	Key Agreement184
9.3.2	Key Derivation185
9.3.3	Encryption Policy187
9.4	Resource Sharing Management189
9.5	Comparison with the PGP's Key-Management Strategy191
9.6	Exposure Evaluation192
9.6.1	Anonymous Accesses192
9.7	Encryption Policy Updates194
9.7.1	Two-Layered Encryption Model195
9.7.2	Over-Encryption196

Contents

- 9.7.3 Collusion Evaluation196
- 9.8 Conclusions.198

References Part II199

Part III Human Computer Interaction (HCI)

- 10 PET-USES 213**
 Erik Wastlund and Peter Wolkerstorfer
 - 10.1 Introduction. 213
 - 10.2 PET-USES in Practice. 215
 - 10.2.1 When to use the PET-USES. 216
 - 10.2.2 How to use the PET-USES. 216
 - 10.3 Conclusions. 217
 - 10.4 Appendix: PET-USES[1.0]. 217
 - 10.4.1 Instructions. 217
- 11 HCI for PrimeLife Prototypes 221**
 Cornelia Graf, Peter Wolkerstorfer, Christina Hochleitner, Erik Wastlund, and Manfred Tscheligi
 - 11.1 Introduction 221
 - 11.2 Overview of HCI challenges. 222
 - 1.2.1 Challenge 1: Limited User Knowledge of PETs. 222
 - 1.2.2 Challenge 2: Technologically Driven Development of PETs. 223
 - 1.2.3 Challenge 3: Understanding PET Related Terms. 223
 - 1.2.4 Challenge 4: Wrong Mental Models of PETs. 223
 - 1.2.5 Challenge 5: Privacy as a Secondary Task 224
 - 1.2.6 Challenge 6: Complex Mechanisms are Hard to Understand 225
 - 11.3 Tackling the Challenges. 225
 - 1.3.1 Limited User Knowledge of PETs. 225
 - 1.3.2 Technologically Driven Development of PETs. 226
 - 1.3.3 Understanding of PET Related Terms. 226
 - 1.3.4 Wrong Mental Models of PETs. 227
 - 1.3.5 Privacy as a Secondary Task 227
 - 1.3.6 Complex Mechanisms are Hard to Understand. 228
 - 14 HCI Activities and Software Development 228
 - 1.4.1 Backup Prototype. 228
 - 1.4.2 Privacy Dashboard. 229
 - 1.4.3 Examples Reflected 230
 - 11.5 Discussion and Outlook. 231

- 12 The Users' Mental Models' Effect on their Comprehension of Anonymous Credentials** 233
 - Erik Wastlund and Simone Fischer-Hiibner
 - 12.1 Introduction 233
 - 12.1.1 Anonymous Credentials 234
 - 12.1.2 Related Work 235
 - 12.2 Performed User Tests 236
 - 12.2.1 Method 236
 - 12.2.2 The Card-Based Approach 238
 - 12.2.3 The Attribute-Based Approach 240
 - 12.2.4 Results of the User Studies 242
 - 12.3 Conclusions & Future Work 242
 - 12.4 Acknowledgments 243

- 13 Trust and Assurance HCI** 245
 - Simone Fischer-Hiibner, Hans Hedbom, and Erik Wastlund
 - 13.1 Introduction 245
 - 13.2 Social Trust Factors 246
 - 13.3 A Trust Evaluation Function 247
 - 13.3.1 Trust Parameters Used 247
 - 13.3.2 Design Principles and Test Results 249
 - 13.3.3 Test Results 251
 - 13.4 The Data Track 253
 - 13.4.1 Use of the Data Track 254
 - 13.4.2 Test Scenarios & Test Setups 256
 - 13.4.3 Results of the Usability Tests 257
 - 13.4.4 Discussion of Data Track Usability Tests 259
 - 13.5 Conclusions 260

- 14 HCI for Policy Display and Administration** 261
 - Julio Angulo, Simone Fischer-Hiibner, Tobias Pulls, and Ulrich Konig
 - 14.1 Introduction 261
 - 14.2 Related Work 263
 - 14.3 User Interfaces for Policy Management and Display 265
 - 14.3.1 Selecting Privacy Preferences 266
 - 14.3.2 The "Send Data?" Dialog 267
 - 14.3.3 Testing the Usability of the "Send Data?" Dialog 273
 - 14.4 Conclusions and Outlook 275

- 15 Privacy Policy Icons** 279
 - Leif-Erik Holtz, Harald Zwingelberg, and Marit Hansen
 - 15.1 Introduction 279
 - 15.2 Motivation for Introducing Privacy Icons 280
 - 15.3 Related Work 280
 - 15.4 PrimeLife Icon Sets 281
 - 15.4.1 PrimeLife Icon Set for General Usage 281

15.4.2	PrimeLife Icon Set for Social Networks	282
15.5	Test Results	282
15.6	An Approach for Handling E-mail Data: Privicons	284
15.7	Conclusions and Outlook	285
References Part III		287
Part IV Policy Languages		
16	Policy Requirements and State of the Art	295
	Carine Bournez and Claudio A. Ardagna	
16.1	Definitions	295
16.1.1	Data Handling Policies	295
16.1.2	Access Control Policies	296
16.1.3	Trust Policies	296
16.2	Legal Requirements	297
16.3	Policy Language Requirements	299
16.3.1	General Design Principles and Expressivity	299
16.3.2	Requirements for Data Handling Policies	300
16.3.3	Requirements for Access Control policies	303
16.3.4	Requirements for Trust policies	305
16.3.5	Other Technical Requirements for PrimeLife	307
16.4	State of the Art	308
16.4.1	Access Control Policy Languages	308
16.4.2	Data Handling Policy Languages	309
16.4.3	Anonymous Credential Systems and Private Information Management	310
17	Matching Privacy Policies and Preferences: Access Control, Obligations, Authorisations, and Downstream Usage	313
	Laurent Bussard, Gregory Neven, and Franz-Stefan Preiss	
17.1	Privacy Specifications: Preferences, Policies, and Sticky Policies	313
17.2	Matching Data Handling	315
17.2.1	Boolean Match	315
17.2.2	Going Further than Boolean Match	316
17.3	Obligations	317
17.3.1	Triggers	318
17.3.2	Actions	319
17.3.3	Enforcement	320
17.4	Authorisations	321
17.5	Downstream Data Handling	321
17.5.1	Structure of Downstream Authorisations	322
17.5.2	Proactive Matching of Downstream Data Handling	323
17.5.3	Lazy Matching of Downstream Data Handling	324
17.6	Conclusion	326

18	Advances in Access Control Policies	327
	Claudio A. Ardagna, Sabrina De Capitani di Vimercati, Gregory Neven, Stefano Paraboschi, Eros Pedrini, Franz-Stefan Preiss, Pierangela Samarati, and Mario Verdicchio	
18.1	Privacy-Preserving Access Control	327
18.1.1	Credentials Enabling Privacy-Preservation	328
18.1.2	A Policy Language for Privacy-Preserving Access Control	329
18.2	Credential Ontologies: Concepts and Relations	331
18.2.1	Abstractions	331
18.2.2	Delegation by Recursion	332
18.3	Dialog Management	333
18.3.1	Policy Sanitisation	334
18.4	Integration into XACML	336
18.4.1	Credential-Based XACML	338
18.4.2	SAML as Claims Language	340
18.4.3	XACML Architecture Extensions	340
18.5	Concluding Remarks	341
19	Legal Policy Mechanisms	343
	Leif-Erik Holtz and Jan Schallabock	
19.1	Introduction	343
19.2	Legal Framework for Processing Personal Data	344
19.3	Gaps in Current Policy Language Approaches	346
19.3.1	XACML	346
19.3.2	P3P	347
19.4	Methodology	348
19.4.1	Looking into Privacy Policies	348
19.4.2	Looking at the Law	349
19.5	Use Cases	350
19.5.1	Online Shopping	350
19.5.2	Social Networking	352
19.6	Results and Further Research	353
20	Policy Implementation in XACML	355
	Slim Trabelsi and Akram Njeh	
20.1	Introduction	355
20.2	Architecture	356
20.2.1	High Level Architecture	356
20.2.2	Detailed Architecture	357
20.3	PPL Policy Language Structure	360
20.3.1	PolicySets, Policy and Rules	361
20.3.2	Credential Requirements	361
20.3.3	Provisional Actions	362
20.3.4	Data Handling Policies	362
20.3.5	Data Handling Preferences	363
20.3.6	Sticky Policies	363

- 20.3.7 Obligations 364
- 20.3.8 Authorisations. 365
- 20.4 PPL Engine Data Model 365
 - 20.4.1 Package pii. 366
 - 20.4.2 Package policy.Impl. 367
 - 20.4.3 Package Credential. 369
 - 20.4.4 Package Obligations. 371
 - 20.4.5 Package StickyPolicy. 372
- 20.5 Conclusion 374

References Part IV. 375

Part V Infrastructures for Privacy and Identity Management

- 21 Privacy for Service Oriented Architectures. 383**
 - Ulrich Pinsdorf, Laurent Bussard, Sebastian Meissner, Jan Schallabock,
and Stuart Short
 - 21.1 Introduction 383
 - 21.2 Requirements for Privacy in SOA. 385
 - 21.2.1 Core Policy Requirements. 386
 - 21.2.2 Privacy Logging Requirements. 387
 - 21.2.3 Requirements for Access to Personal Information. 389
 - 21.2.4 Cross-Domain-Specific Requirements. 389
 - 21.2.5 Requirements for Additional Mechanisms. 390
 - 21.3 Abstract Framework Addressing the Lifecycle of Privacy
Policies in SOAs 392
 - 21.3.1 Privacy Issues Arising from SOA. 394
 - 21.3.2 Abstract Protocol. 395
 - 21.3.3 PII Provider. 398
 - 21.3.4 PII Consumer. 400
 - 21.3.5 Matching Abstract Framework with SOA Requirements .402
 - 21.4 Policy Composition. 404
 - 21.4.1 Policy Composition Scenario. 405
 - 21.4.2 Privacy Policy Composition Challenges. 406
 - 21.4.3 Data-Centric Architecture for Privacy Enforcement. 408
 - 21.4.4 Conclusion. 410
 - 21.5 Outlook and Open Issues. 411
- 22 Privacy and Identity Management on Mobile Devices: Emerging
Technologies and Future Directions for Innovation. 413**
 - Marc-Michael Bergfeld and Stephan Spitz
 - 22.1 The Status: Privacy and Identity Management on Smart Mobile
Devices. 413
 - 22.2 The Changing Context (I): Multiple Partial Identities across
Devices. 414

- 22.3 The Changing Context (II): Multiple Identity Providing Stakeholders Along an Increasingly Dynamic Mobile Services Value Chain. 415
- 22.4 Technologies for Identity Management and Privacy Enhancement: Secure Elements. 417
- 22.5 Present Secure Element Technologies: UICCs and Stickers. 420
 - 22.5.1 The Universal Integrated Circuit Card (UICC) and the Smart Card Web Server. 420
 - 22.5.2 The Sticker as Example for Static Mobile Service Identities. 421
- 22.6 Emerging Secure Element Technologies: Trusted Execution Environments and the Privacy Challenge. 422
- 22.7 Technologies for Secure and Dynamic Mobile Services and the Privacy Challenge in Highly Dynamic Environments. 424
- 22.8 Contributions of the PrimeLife Project for the Advancement of Technologies in the Field. 426
- 22.9 The Privacy Challenge in Mobile Services and Future Directions for Innovation. 428
- 23 Privacy by Sustainable Identity Management Enablers. 431**
 - Sascha Koschinat, Gokhan Bal, Christian Weber, and Kai Rannenberg
 - 23.1 Introduction. 431
 - 23.2 Economic Valuation Approach for Telco-Based Identity Management Enablers. 432
 - 23.2.1 Description of the Baseline Option and Feasible Delta Options. 434
 - 23.2.2 Identification of each Stakeholder's Costs and Benefits Based on Delta Scenarios in Comparison to the Baseline Scenario. 436
 - 23.2.3 Selection of Key Costs and Benefits for each Stakeholder 439
 - 23.2.4 Mapping of each Stakeholder's Key Cost and Benefits on IdM Service Provider by Cause-Effect Chains. 439
 - 23.2.5 Clustering of Mapped IdM Service Provider Costs and Benefits. 440
 - 23.2.6 Assessment and Aggregation of Clustered IdM Service Provider costs and Benefits. 443
 - 23.2.7 Visualisation of Aggregated IdM Service Provider Costs and Benefits. 445
 - 23.3 Description of the Identity Management Scenarios. 445
 - 23.3.1 Authentication. 446
 - 23.3.2 Privacy Policy Enforcement 447
 - 23.4 Related Work. 451
 - 23.5 Summary and Future Work. 452
- References Part V. 453**

Part VI Privacy Live

24 Open Source Contributions 459
 Jan Camenisch, Benjamin Kellermann, Stefan Kopsell, Stefano
 Paraboschi, Franz-Stefan Preiss, Stefanie Potzsch, Dave Raggett,
 Pierangela Samarati, and Karel Wouters

24.1 Introduction 459

24.2 Social Software 460

 24.2.1 Clique - Privacy-Enhanced Social Network Platform 460

 24.2.2 Scramble! - Audience Segregation by Encryption 461

 24.2.3 Privacy-Awareness Support for Forum Users: Personal
 Data MOD 462

 24.2.4 Privacy-Enhancing Selective Access Control for Forums . 464

24.3 Duddle - *Privacy-enhanced* Web 2.0 Event Scheduling 464

24.4 The Privacy Dashboard 466

24.5 Privacy in Databases 470

 24.5.1 Pri-Views - Protecting Sensitive Values by Fragmentation 470

 24.5.2 Over-Encrypt 471

24.6 Anonymous Credentials 472

 24.6.1 Identity Mixer Crypto Library 472

 24.6.2 Components for a Privacy-Preserving Access Control
 System 473

24.7 Conclusion 474

25 Contributions to Standardisation 479
 Hans Hedbom, Jan Schallabock, Rigo Wenning, and Marit Hansen

25.1 Introduction 479

25.2 Standardisation in ISO/IEC JTC 1/SC 27/WG 5 480

 25.2.1 ISO 24760 - Framework for Identity Management 481

 25.2.2 Introducing Privacy Protection Goals to ISO 29101
 Privacy Reference Architecture 482

25.3 Web Privacy 485

 25.3.1 Workshop on Access Control Application Scenarios 486

 25.3.2 Workshop on Privacy for Advanced Web APIs 488

 25.3.3 Workshop on Privacy and Data Usage Control 489

 25.3.4 Workshop on Internet Privacy 490

25.4 PrimeLife's Contributions to Standardisation in IETF 491

25.5 Conclusion and Outlook 491

26 Best Practice Solutions 493
 Marit Hansen

26.1 Introduction 493

26.2 Recommendations to Industry 493

 26.2.1 Data Minimisation by Pseudonyms and Private
 Credentials 494

 26.2.2 Improvement of Privacy Functionality in Social Media .. 494

- 26.2.3 Better Protection of the User's Privacy on the Web. 496
- 26.2.4 Better Information of Users on Privacy-Relevant Issues
on the Web. 496
- 26.3 Recommendations to Policy Makers. 497
 - 26.3.1 Clear Guidelines for System Developers and Data
Controllers. 498
 - 26.3.2 Incentives and Sanctions. 499
 - 26.3.3 Development of Law. 499
- References Part VI** 503
- 27 PrimeLife's Legacy**. 505
Jan Camenisch and Marit Hansen
- Index** 507